Abstract

Cryptography-based methods and apparatus for secure information processing are disclosed that are particularly efficient in terms of the computational resources required, and thus implementable in mobile telephones, personal digital assistants (PDAs) or other lightweight processing devices. A setup procedure is performed to permit interactions of a designated type, e.g., secure mobile gaming interactions, to be carried out between participants, e.g., one or more players and a casino. A given participant initiates a particular interaction with another participant by sending to that participant initiation information based at least in part on one or more results of the setup procedure. The other participant in turn sends response information back to the given participant, and the interaction then continues with one or more rounds each involving one or more decisions committed to by each participant. Transcripts of the interaction can be used to determine rights of the first and second participants in a publicly verifiable manner, with the rights being based upon particular results of the interaction. The invention may be configured to permit arbitrary disconnection of the lightweight devices, and provides the advantages of public verifiability, fairness and robustness. Although the invention is particularly well suited for use in secure mobile gaming applications, it is also applicable to other secure information processing applications, including contract signing and fair exchange of digital signatures.